HENSEL'S LEMMA FOR NONCOMMUTATIVE RINGS

JOSHUA MUNDINGER

ABSTRACT. We prove a version of Hensel's lemma for lifting solutions of a polynomial equation in a noncommutative ring.

1. Noncommutative Hensel's Lemma

Theorem 1.1. *Let R be a commutative ring and $f \in R[t]$ such that f and f' generate the unit ideal of $R[t]$. Suppose that A is an associative R-algebra and I is a two-sided ideal of A such that A is I-adically complete.*

If $x_0 \in A/I$ satisfies $f(x_0) = 0$, then

(1) *there is a lift $x \in A$ of x_0 such that $f(x) = 0$;*
(2) *if y is another lift of x_0 such that $f(y) = 0$, then $y = uxu^{-1}$ for $u \in 1 + I$.*

The proof of existence is standard and no different from the commutative case. The proof of uniqueness here is due to Dima Arinkin.

Proof. Since A is complete, the general statement reduces to the case when $I^2 = 0$; thus assume $I^2 = 0$. The hypothesis $(f, f') = 1$ implies $f'(x_0)$ is invertible in A/I.

First, we show that a lift x of x_0 such that $f(x) = 0$ exists. Suppose that $\tilde{x}$ is any lift of x_0. Since $f'(x_0)$ is invertible in A/I, also $f'(\tilde{x})$ is invertible in A. Define

$$x = \tilde{x} - f'(\tilde{x})^{-1} f(\tilde{x}).$$

Note that $f(\tilde{x}) \in I$. Since $\tilde{x}$ commutes with any polynomial in $\tilde{x}$, and $I^2 = 0$, we have by Taylor expansion

$$f(x) = f(\tilde{x}) + f'(\tilde{x}) \left(-f'(\tilde{x})^{-1} f(\tilde{x}) \right) = 0.$$

Thus a desired lift x exists.

Now suppose that y is another lift of x_0 to a zero of f. Set $h = y - x$; if $u = 1 + v$ for $v \in I$, then

$$uxu^{-1} = x + [v, x],$$

so the goal is to show that $h = [v, x]$ for some $v \in A$. This claim depends only on h and x, so we may replace A with the subalgebra A_0 generated by h and x. This algebra is spanned by expressions x^α and $x^\alpha h x^\beta$, as h is in a two-sided square-zero ideal. Then $J = [x, A_0]$ is a two-sided ideal in A_0: $[x, x] = 0$ so $[x, A_0] \subseteq I$; $[x, A_0]$ is closed under multiplication by x on both sides, and also by multiplication by h on both sides since $hI = Ih = 0$. The ring A_0/J is commutative, so

$$0 = f(x + h) - f(x) = f'(x)h \mod J.$$

As $f' \in R[t]/(f)$ is a unit, $f'(x)$ is invertible in A_0/J, so $h = 0 \mod J$. Thus $h \in [x, A_0]$, as desired. ∎

Date: November 30, 2024.

Remark 1.2. Davis considered a version of uniqueness when $A = M_n(\mathbb{Z}_p)$ is a matrix ring over the p-adic integers, and gave an explicit formula for v such that $[x, v] = h$ in terms of x, h, f [Dav68, Theorem 2].

Example 1.3. If $(f, f') \neq 1$ then lifts may not be unique up to conjugation. See e.g. [McD84, Exercise V.D.17] and `https://mathoverflow.net/questions/317704`.

There is also a cohomological proof of Theorem 1.1. We give one for monic f.

Cohomological proof of Theorem 1.1 for monic f. Suppose that B is an R-algebra which is projective as an R-module. If $B \to A/I$ is an R-algebra homomorphism and $I^2 = 0$, then the obstructions to lifting $B \to A/I$ to a R-algebra homomorphism lie in $\mathrm{HH}^2(B/R, I)$ and lifts up to conjugation are a torsor over $\mathrm{HH}^1(B/R, I)$, where

$$\mathrm{HH}^i(B/R, I) = \mathrm{Ext}^i_{B \otimes_R B^{op}}(B, I)$$

are the Hochschild cohomology groups for $i \geq 0$.[1]

Suppose that f is monic and $(f', f) = 1$. Then $B = R[t]/(f)$ is a free R-module. Now $B \otimes_R B^{op} = R[t, t']/(f(t), f(t'))$. If we set $h = t' - t$, then we have

$$f(t + h) - f(t) = hf'(t) + h^2 g(t, h)$$

for some g. Now $f'(t)$ is a unit modulo f, so the defining ideal of $B \otimes_R B$ is

$$(f(t), f(t + h)) = (f(t), h(1 + hc(t, h)))$$

for some $c(t, h) \in R[t, h]$. By the Chinese Remainder Theorem,

$$B \otimes_R B^{op} = B[h]/(h) \times B[h]/(1 + hc(t, h)).$$

Thus the diagonal bimodule B is a projective bimodule, so $\mathrm{HH}^i(B/R, -) = 0$ for $i > 0$. Thus a homomorphism $R[t]/(f) \to A/I$ has a lift to $R[t]/(f) \to A$, unique up to conjugation. □

2. Applications

Example 2.1 (Idempotent lifting)**.** Let $f(t) = t^2 - t \in \mathbb{Z}[t]$. Then $f'(t) = 2t - 1$ has $(2t - 1, t^2 - t) = 1$, for

$$(2t - 1)^2 - 4(t^2 - t) = 1.$$

Theorem 1.1 applies and shows that if A is a ring, $I \subseteq A$ a two-sided ideal such that A is I-adically complete, then any idempotent $e_0 \in A/I$ lifts to A, uniquely up to conjugation by $1 + I$.

The uniqueness of idempotent lifting up to conjugation is well-known [Eti+11, Proposition 7.3], [Row91, Corollary 1.1.28].

Example 2.2 (Brauer lifting)**.** Let $(R, \mathfrak{m})$ be a complete local ring of mixed characteristic $(0, p)$. Let $A = M_n(R)$, $I = \mathfrak{m}A$, and $f(t) = t^e - 1$ where $(e, p) = 1$. Then $f'(t) = et^{e-1}$ and $e \in R^\times$, so (f', f) is the unit ideal in $R[t]$. Thus, if $g_0 \in M_n(R/\mathfrak{m})$ has $g_0^e = 1$ there is a lift to $g \in M_n(R)$ such that $g^e = 1$, unique up to conjugation. Thus we can define the Brauer trace

$$tr_{\mathrm{Br}}(g_0) = tr(g) \in R.$$

[1]If B is not a projective R-module, then more care is necessary to define the Hochschild cohomology groups and establish the link to deformation theory.

Since the lift is unique up to conjugation, the trace of a lift does not depend on the choice of lift, and agrees with Brauer's definition of summing multiplicative lifts of the eigenvalues of g_0.

In this case, the existence and uniqueness of such a lift also follows from the vanishing of the group cohomology $H^i(\langle g_0 \rangle, M_n(k))$ for $i \in \{1, 2\}$, as noted in [Ser77, Exercise 15.9].

References

[Dav68] Davis, R. W. "Certain matrix equations over rings of integers". In: *Duke Math. J.* 35 (1968), pp. 49–59.

[Eti+11] Etingof, P., Golberg, O., Hensel, S., Liu, T., Schwendner, A., Vaintrob, D., and Yudovina, E. *Introduction to representation theory.* Vol. 59. Stud. Math. Libr. With historical interludes by S. Gerovitch. American Mathematical Society, 2011.

[McD84] McDonald, B. R. *Linear algebra over commutative rings.* Vol. 87. Monogr. Textbooks Pure Appl. Math. Marcel Dekker, Inc., 1984.

[Row91] Rowen, L. H. *Ring theory.* Student edition. Academic Press, Inc., 1991.

[Ser77] Serre, J.-P. *Linear representations of finite groups.* Trans. by Scott, L. L. Vol. 42. Graduate Texts in Mathematics. Springer-Verlag, 1977.

University of Wisconsin-Madison, Madison, WI

Email address: jmundinger@wisc.edu